UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA

Case No. _____

JAMES MOORE, Individually And On Behalf Of All Others Similarly Situated, Plaintiff, v. MANAGED CARE OF NORTH AMERICA, INC., Defendant.	CLASS ACTION **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiff James Moore ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action against Managed Care of North America, Inc., d/b/a MCNA Dental Plans ("MCNA Dental" or "Defendant"). Plaintiff makes the following allegations, except as to allegations specifically pertaining to Plaintiff, upon information and belief based on, among other things, the investigation of counsel and review of public documents.

I. NATURE OF THE ACTION

1. Plaintiff brings this class action against MCNA Dental due to its failure to properly secure and safeguard sensitive and confidential personally identifiable information ("PII"), including names, addresses, telephone numbers, email addresses, driver's license numbers, driver's license numbers, and dates of birth, and personal health information ("PHI") of its current and former customers (PII and PHI together, "Personal Information"). Defendant's wrongful disclosure has harmed Plaintiff and the Classes (defined below), which include millions of people.

2. Medical and financial records represent the most sensitive information available concerning a person's private affairs. These records reveal intimate and personal aspects of the human condition, such as illnesses that might carry social stigma and details about substance abuse, family planning and mental health. Congress has passed legislation under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") in order to protect this highly confidential data, because in the wrong hands, bad actors may target and exploit the most sensitive and vulnerable populations among the public.

3. MCNA Dental is the nation's largest dental insurer for government subsidized Medicaid and Children's Health Insurance Programs ("CHIP"), meaning that many insureds are low-income or belong to other vulnerable populations. MCNA Dental collected and retained the personal information and health information of its customers, including Plaintiff and Class Members in connection with providing dental insurance, dental care, or related services or products (collectively, "Dental Services").

4. MCNA Dental had an obligation to safeguard this information. On May 26, 2023, MCNA Dental confirmed that it had suffered a ransomware attack that disrupted its computer systems ("Data Breach"). MCNA Dental detected the attack on March 6, 2023, and waited more than eleven weeks before informing the public. Indeed, Plaintiff did not receive a notification letter until May 26, 2023.

5. MCNA Dental knew or should have known of the increasing number of well-publicized data breaches that have occurred in the United States. And yet, MCNA Dental failed to adequately secure and upgrade its systems, allowing another breach to occur, this time compromising consumer Personal Information.

6. Plaintiff and members of the Classes ("Class Members") entrusted MCNA Dental with their sensitive and valuable Personal Information. Plaintiff and Class Members did not know that MCNA Dental's data security was so inadequate. They did not expect that by obtaining an insurance policy through MCNA Dental so they could obtain dental benefits, they would suffer serious injury that would last for years after the insurance coverage.

7. MCNA Dental has caused harm to Plaintiff and Class Members by collecting, using, and maintaining their Personal Information for its own economic benefit but utterly failing to protect that information: MCNA Dental did not maintain adequate security systems, did not properly archive Personal Information, allowed access by third parties, and did not implement sufficient security measures.

8. Plaintiff brings this action on behalf of all persons in the United States whose Personal Information was compromised as a result of Defendant's failure to: (a) adequately protect its customers' Personal Information; (b) warn customers of its inadequate information security practices; and (c) effectively secure hardware, data, and information systems through reasonable and effective security procedures. Defendant's conduct constitutes negligence that proximately caused damages to Plaintiff and Class Members.

9. Plaintiff and Class Members have suffered injury as a direct and proximate result of Defendant's conduct. These injuries include: (a) lost or diminished value of Personal Information, a form of property that MCNA Dental obtained from Plaintiff and Class Members; (b) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft and other unauthorized use of their Personal Information; (c) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (d) the continued and certain increased risk that unauthorized persons will access and abuse Plaintiff's and

Class Members' unencrypted Personal Information that is available on the dark web; (e) the continued and certain increased risk that the Personal Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake appropriate and adequate measures to protect the Personal Information; (f) invasion of privacy; and (g) theft of their Personal Information and the resulting loss of privacy rights in that information.

10. As a direct and proximate result of MCNA Dental's breach of confidence and failure to protect the Personal Information, Plaintiff and Class Members have been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuses of their Personal Information; ongoing monetary loss and economic harm; loss of value of privacy and confidentiality of the stolen Personal Information; illegal sales of the compromised Personal Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. §1332(d)(2) because: (1) this is a class action involving more than 1,000 class members; (2) minimal diversity is present as the Plaintiff is a citizen of Arkansas while Defendant is a citizen of Florida, and thus Defendant is a citizen of a state different from that of at least one Class Member; and (3) the amount in controversy exceeds the sum of $5,000,000, exclusive of interest and costs.

12. This Court has personal jurisdiction over MCNA Dental because MCNA Dental is a citizen of Florida, and the wrongful acts alleged in this Complaint were committed in Florida, among other venues. MCNA Dental has intentionally availed itself of this jurisdiction by conducting operations here, contracting with companies in this District, and marketing and selling its products and services in Florida.

13. Venue is proper in this District pursuant to: (1) 28 U.S.C. §1391(b)(2) in that a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District, and 28 U.S.C. §1391(d) because the transactions giving rise to the claims occurred in Miramar, Florida; and (2) 28 U.S.C. §1391(b)(3) in that Defendant is subject to personal jurisdiction in this District.

III. INJURY TO PLAINTIFF AND CLASS MEMBERS

14. Plaintiff is an individual who had his Personal Information compromised in the Data Breach and brings this action on behalf of himself and all those similarly situated both across the U.S. and within their state or territory of residence.

15. Because MCNA Dental has exclusive knowledge of what information was compromised for each individual Class Member, Plaintiff reserves the right to supplement his allegations with additional facts and injuries as they are discovered.

16. Plaintiff has suffered actual injury and one or more concrete (real and not abstract), imminent and particularized injuries described below as a direct and proximate result of MCNA Dental's known deficient data security and failure to protect Plaintiff's Personal Information, as well as MCNA Dental's concealment of the same, that allowed unauthorized access to Plaintiff's Personal Information.

17. Had MCNA Dental disclosed that it disregarded its duty to protect Plaintiff's Personal Information, or otherwise had insufficient security measures to safeguard and protect Plaintiff's Personal Information from unauthorized access, Plaintiff would have taken this into account in making his insurance purchasing decisions. Instead of purchasing MCNA Dental products and services, Plaintiff could have purchased products and services from competing providers that protected Plaintiff's Personal Information.

18. Had Plaintiff and the Classes known that purchasing MCNA Dental products and services, creating MCNA Dental accounts, or providing Personal Information to MCNA Dental would result in their Personal Information being compromised and exfiltrated, Plaintiff and the Classes would not have purchased the products or services, or would have paid less for them, or would not have provided some or all of their Personal Information to MCNA Dental. Thus, Plaintiff and the Classes significantly overpaid based on what the products were represented to be compared to what Plaintiff and the Classes actually received.

19. In addition to actual, present, concrete, and current injuries described below, because of MCNA Dental's actions and omissions, Plaintiff and Class Members suffered, and will continue to suffer perpetual emotional distress, worry, other emotional or psychological harm, and well-founded fear that additional, realistic, objectively-reasonable, threatened, impending, sufficiently imminent harm in the form of identity theft or fraud will occur in the future.

20. The Data Breach was the product of an intentional criminal act to gain access to the data. It was the result of a sophisticated, intentional, and malicious attack by professional cybercriminal hackers and was not the result of an accidental disclosure by an MCNA Dental employee. Thus, there is an increased and substantial risk that the victims will experience identity theft or fraud that is sufficiently imminent.

21. On information and belief, LockBit, one of the world's most active ransomware groups, claimed the cyberattack on MCNA Dental on March 7, 2023, when the group published data samples stolen from the healthcare provider. LockBit threatened to publish 700GB of sensitive, confidential information they exfiltrated from MCNA Dental's networks unless they were paid $10 million. On April 7, 2023, LockBit released all data on its website, making it available for download by anyone.

22. Upon information and belief, the Personal Information stolen in the Data Breach included information such as social security numbers, birth dates, financial information, and full names that thieves are likely to use to perpetrate identity theft or fraud now or at any time in the future.

23. The concreteness of the injury included traditional harms such as monetary harm recognized as a basis for a lawsuit in American courts.

24. Plaintiff has also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Personal Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Personal Information, illegal sales of the compromised Personal Information, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, and lost work time.

25. The dark web is a portion of the internet that facilitates criminal activity worldwide and functions as an underground illicit market for the sale of sensitive stolen data and illegal products such as drugs, weapons, and counterfeit money.

26. There are strong indications that the Personal Information exfiltrated from MCNA Dental's network has been published and is still being offered for download and/or sale on underground marketplaces.

IV. PARTIES

A. Plaintiff

27. Plaintiff James Moore ("Plaintiff") resides in Rogers, Arkansas.

28. Plaintiff received Dental Services from MCNA Dental. As a condition of receiving Dental Services, Plaintiff was required to provide his Personal Information to MCNA Dental. MCNA Dental retained and stored Plaintiff's PII and PHI on its computer systems, including the systems affected by the Data Breach.

29. Plaintiff takes great care to protect his Personal Information. Had Plaintiff known that MCNA Dental does not adequately protect the PII/PHI in its possession, he would not have obtained services from MCNA Dental or agreed to provide them with his Personal Information.

30. Plaintiff, like all Class Members, received a written form of a notice from Defendant dated May 26, 2023. Plaintiff, however, appears to have already been the target of insurance-related crimes during the period between when the Data Breach occurred and when he had received the notice. Indeed, since the Data Breach occurred Plaintiff has had two insurance claims related to medical services denied by Medicaid, despite the fact that insurance claims submitted to Medicaid from the same medical provider had never been denied in the past. Upon receiving the claim denials, Plaintiff contacted the Social Security Administration who advised Plaintiff that his insurance information could have been accessed in the Data Breach and corrupted as a result, leading to the denial of his claims. Plaintiff has expended, and will continue to expend, significant time appealing

the insurance claim denials, to avoid having to pay out of pocket for the medical services, which should have been covered in the first instance by Medicaid.

31. As a direct and proximate result of the breach, Plaintiff has made reasonable efforts to mitigate the impact of the Data Breach. Plaintiff has spent time attempting to freeze his credit report, monitoring his account information and credit reports for fraudulent activity, contacting his Medicaid and the Social Security Administration, utilizing credit monitoring services, and taking other steps to mitigate or ameliorate the damages caused by MCNA Dental's misconduct.

32. Plaintiff is very concerned about identity theft and the consequences of such theft and fraud resulting from the Data Breach.

33. Plaintiff suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (a) damage to and diminution in the value of Plaintiff's Personal Information, a form of property that MCNA Dental obtained from Plaintiff; (b) violation of Plaintiff's privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

34. As a result of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address the harms caused by the Data Breach. As a result of the Data Breach, Plaintiff is and will continue to be at increased risk of identity theft and fraud for years to come.

B. Defendant

35. Managed Care of North America, Inc., d/b/a MCNA Dental Plans, is a private, for-profit dental benefits management company established in 1990 with its principal place of business in Miramar, Florida. MCNA Dental offers long-term Medicare/Medicaid, CHIP, and commercial plans for private employers, individuals, and families.

V. FACTUAL BACKGROUND

A. MCNA Dental Is a Prominent Dental Benefits Management Company Throughout the United States

36. MCNA Dental is the largest dental insurer in the nation for government-sponsored Medicare/Medicaid and CHIP, with over five million members across eight states. MCNA Dental also offers dental plans and services for private employers, individuals, and families throughout the United States.

37. MCNA Dental's website contains a Notice of Privacy Practices.[1] In its Notice of Privacy Practices, MCNA Dental states, "[o]ne of our strengths is our ability to administer dental plans in an effective and innovate manner while safeguarding our members' protected health information."[2] MCNA Dental also promises its patients that it is "committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" and states that it is required by law to "maintain the privacy and security of your protected health information."[3]

38. MCNA Dental also describes in its Privacy Policy the limited specific instances when it shares PII/PHI and says that it will not otherwise share patients' information "unless you tell us we can in writing."[4]

---

[1] *See Our Privacy Practices*, MCNA Dental, https://www.mcna.net/en/privacy (updated June 2018)

[2] *Id.*

[3] *Id.*

[4] *Id.*

39. MCNA Dental claims to protect PII/PHI, including names, addresses, telephone numbers, and Social Security numbers, "in all formats including electronic, written and oral information."[5]

40. MCNA Dental promises to "let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[6]

41. MCNA Dental's website also touts its management information system, DentalTrac™ as "ensuring[ing] the security and availability of data through strict adherence to HIPAA requirements, keeping MCNA Dental in full compliance with all federal regulations."[7] MCNA Dental's website also states that:

a) "MCNA has successfully completed an independent, third-party SOC 2 audit of the processes and controls that ensure the security and availability of our information management systems and data."

b) "DentalTrac™ is hosted across multiple geographically dispersed, military grade, secure, and state-of-the-art data centers. All hardware components are fully mirrored in every location guaranteeing high scalability and business continuity to support our current and future needs."

c) "The DentalTrac™ system has been based on HIPAA-compliant solutions. MCNA is fully committed to ensuring a clear and easy path to HIPAA readiness well ahead of federally mandated compliance deadlines." [8]

---

[5] *Id.*

[6] *Id.*

[7] *Company Overview*, MCNA Dental, https://www.mcnala.net/en/company-overview (last visited June 28, 2023)

[8] *Our Technology*, MCNA Dental, https://www.mcna.net/en/technology/ (last visited June 28, 2023).

B. The Data Breach and MCNA Dental's Delayed Disclosure

42. On May 26, 2023, MCNA Dental confirmed they had suffered a ransomware attack that disrupted their computer systems. MCNA Dental purportedly detected the attack on March 6, 2023, blocked the unauthorized access, and launched an investigation to determine the nature and scope of the breach.

43. MCNA Dental confirmed that the hackers gained access to part of its systems and removed copies of Personal Information between February 26, 2023 and March 7, 2023. MCNA Dental concluded that the Data Breach impacted over 8,923,662 people, encompassing patients, parents, guardians, and/or guarantors.

44. The stolen information included names, addresses, dates of birth, emails, social security numbers, driver's license numbers and/or other government-issued ID numbers, health insurance information (plan information, insurance company, member number, Medicaid/Medicare ID numbers), care for teeth or braces (visits, dentist name, doctor name, past care, x-rays/photos, medicines, and treatment), and bills and insurance claims. Some of the stolen information was for a parent, guardian, or guarantor. Complimentary identity theft protection services were offered to individuals for one year.

45. Plaintiff and other Class Members received a letter dated May 26, 2023, stating *inter alia* the following:

> **What happened?** On March 6, 2023, MCNA became aware that an unauthorized party was able to access certain MCNA systems. Upon discovery the same day, MCNA took immediate steps to contain the threat and engaged a third-party forensic firm to investigate the incident and assist with remediation efforts. MCNA subsequently discovered that certain systems within the network may have been infected with malicious code. Through its investigation, MCNA determined that an unauthorized third party was able to access certain systems and remove copies of some personal information between February 26, 2023 and March 7, 2023. MCNA undertook an extensive review to determine what data may have been

> impacted. As a result of this review, which was completed on May 3, 2023, it appears that your personal information may have been involved.
>
> **What information was involved?** Personal information that may have been involved included: (1) demographic information to identify and contact you, such as full name, date of birth, address, telephone and email; (2) Social Security number; (3) driver's license number or government-issued identification number; (4) health insurance information, such as name of plan/insurer/government payor, member/Medicaid/Medicare ID number, plan and/or group number; and (5) information regarding dental/orthodontic care. **Not all data elements were involved for all individuals.**
>
> **What we are doing.** MCNA takes privacy and security very seriously. As soon as we discovered the incident, we promptly launched a forensic investigation, took steps to mitigate and remediate the incident and to help prevent further unauthorized activity, and contacted law enforcement. In response to this incident, we have enhanced our security controls and monitoring practices as appropriate, to minimize the risk of any similar incident in the future.

46. However, not every impacted individual will receive a notice, as MCNA Dental does not have current addresses for everyone. Accordingly, the organization published a substitute notice on IDX, which will stay online for 90 days. On that notice, MCNA Dental identified a list of over a hundred healthcare providers indirectly impacted by this incident. It is unclear if those entities will publish separate notices of the Data Breach.[9]

C. MCNA Dental Violated HIPAA's Requirements to Safeguard Data

47. Defendant had duties to ensure that all information it collected and stored was secure, and that it maintained adequate and commercially reasonable data security practices to ensure the protection of plan members' Personal Information.

48. Defendant is covered by HIPAA (*see* 45 C.F.R. §160.102) and as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164,

[9] *Notice of Data* Breach, MCNA Dental, https://response.idx.us/MCNA-Information/ (last visited June 28, 2023).

Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

49. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. §160.103.

50. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

51. HIPAA requires that Defendant implements appropriate safeguards for this information.

52. HIPAA requires that Defendant provide notice of a breach of unsecured protected health information, which includes protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons – *i.e.*, non-encrypted data. Such notice is to be provided without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

53. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e-PHI and comply with the risk analysis requirements

of the Security Rule." *See* U.S. Department of Health & Human Services, Security Rule Guidance Material.[10] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-PHI." *See* U.S. Department of Health & Human Services, Guidance on Risk Analysis.[11]

54. Should a health care provider experience an unauthorized disclosure, it is required to conduct a four-factor Risk Assessment (HIPAA Omnibus Rule: "A covered entity or business associate must now undertake a four-factor risk assessment to determine whether or not PHI has been compromised and overcome the presumption that the breach must be reported."). The four-factor risk assessment focuses on:

(1) the nature and extent of the Personal Information involved in the incident (*e.g.*, whether the incident involved sensitive information like Social Security numbers or infectious disease test results);

(2) the recipient of the PHI;

(3) whether the PHI was actually acquired or viewed; and

(4) the extent to which the risk that the PHI was compromised has been mitigated following unauthorized disclosure (*e.g.*, whether it was immediately sequestered and destroyed).[12]

---

[10] *Security Rule Guidance Material*, U.S. Dep't Health & Humand Svcs., http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html (last visited Jun 28, 2023).

[11] *Guidance on Risk Analysis*, U.S. Dep't Health & Humand Svcs., https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html (last visited June 28, 2023).

[12] 78 Fed. Reg. 5641-46; *see also* 45 C.F.R. §164.304.

55. The HIPAA Breach Notification Rule, 45 C.F.R. §§164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.

56. Despite these requirements, Defendant failed to comply with its duties under HIPAA and its own Privacy Practices. Indeed, Defendant failed to:

a) Maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b) Adequately protect Plaintiff's and the Class Members' Personal Information;

c) Ensure the confidentiality and integrity of electronically protected health information created, received, maintained, or transmitted, in violation of 45 C.F.R. §164.306(a)(1);

d) Implement technical policies and procedures for electronic information systems that maintain electronically protected health information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 C.F.R. §164.312(a)(1);

e) Implement adequate policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 C.F.R. §164.308(a)(1)(i);

f) Implement adequate procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports, in violation of 45 C.F.R. §164.308(a)(1)(ii)(D);

g) Protect against reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy rules

regarding individually identifiable health information, in violation of 45 C.F.R. §164.306(a)(3);

h) Take safeguards to ensure that Defendant's business associates adequately protect Personal Information;

i) Conduct the four-factor Risk Analysis following the Data Breach;

j) Properly send timely notice to Plaintiff and the Classes pursuant to 45 C.F.R. §§164.400-414;

k) Ensure compliance with the electronically protected health information security standard rules by its workforce, in violation of 45 C.F.R. §164.306(a)(4); and/or

l) Train all members of its workforce effectively on the policies and procedures with respect to protected health information as necessary and appropriate for the members of its workforce to carry out its functions and to maintain security of protected health information, in violation of 45 C.F.R. §164.530(b).

57. Defendant failed to comply with its duties under HIPAA and its own privacy policies despite being aware of the risks associated with unauthorized access of members' Personal Information.

D. MCNA Dental Was on Notice That Highly Valuable Personal Information of Its Patients Could Be Breached

58. Defendant was, or should have been, aware that it was collecting highly valuable data, for which Defendant knew, or should have known, there is an upward trend in data breaches

in recent years.[13] Accordingly, Defendant was on notice of the harms that could ensue if it failed to protect patients' data.

59. As early as 2014, the Federal Bureau of Investigation ("FBI") alerted the healthcare industry that they were an increasingly preferred target of hackers, stating "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)" so that these companies can take the necessary precautions to thwart such attacks.[14]

60. Personal Information is a valuable commodity to identity thieves. Compromised Personal Information is traded on the "cyber black-market." As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen credit card numbers, Social Security numbers, and other Personal Information directly on various dark web[15] sites making the information publicly available.[16]

---

[13] *Healthcare Data Breach Statistics*, HIPAA Journal, https://www.hipaajournal.com/healthcare-data-breach-statistics/ (last visited June 28, 2023) ("Our healthcare data breach statistics clearly show there has been an upward trend in data breaches over the past 14 years, with 2021 seeing more data breaches reported than any other year since records first started being published by [the U.S. Department of Health and Human Services' Office for Civil Rights].").

[14] Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, Reuters (Aug. 20, 2014) http://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[15] The dark web refers to encrypted content online that cannot be found using conventional search engines and can only be accessed through specific browsers and software. MacKenzie Sigalos, *The dark web and how to access it*, CNBC (Apr. 14, 2018), https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html.

[16] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian (Dec. 6, 2017) https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/; Charles McFarland et al., *The Hidden Data Economy*, at 3, https://partners.trellix.com/enterprise/en-us/assets/reports/rp-hidden-data-economy.pdf (last visited June 28, 2023).

61. Further, medical databases are particularly high value targets for identity thieves. According to one report, a stolen medical identity has a $50 street value on the black market, whereas a Social Security number sells for only $1.[17]

E. Consequences of the Data Breach for Consumers

62. Plaintiff and Class Members have suffered actual harm and will continue to be harmed as a result of MCNA Dental's conduct. MCNA Dental failed to institute adequate security measures and neglected system vulnerabilities that led to the Data Breach. MCNA Dental's failure to keep Plaintiff's and Class Members' Personal Information secure has severe ramifications. Given the sensitive nature of the Personal Information stolen in the Data Breach – names, addresses, dates of birth, Social Security numbers, driver's license numbers and/or other government-issued ID numbers, health insurance information, Medicaid/Medicare ID numbers, and medical records – hackers can commit identity theft, financial fraud, and other identity-related fraud against Plaintiff and Class Members now and into the indefinite future. Plaintiff and Class Members may be subject to blackmail from nefarious actors concerning the disclosure of their medical records. As a result, Plaintiff and Class Members have suffered injury and face an imminent and substantial risk of further injury including identity theft and related cybercrimes due to the Data Breach.

63. Plaintiff's stolen Personal Information may now be circulating on the dark web and it is highly valuable. Malicious actors use Personal Information to, among other things, gain access to consumers' bank accounts, social media, and credit cards. Malicious actors can also use consumers' Personal Information to open new financial accounts, open new utility accounts, obtain

[17] *Study: Few Aware of Medical Identity Theft Risk*, Claims Journal (June 14, 2012), https://www.claimsjournal.com/news/national/2012/06/14/208510.htm.

medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create synthetic identities.

64. Theft of Social Security numbers also creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of their social security number, and a new social security number will not be provided until after the harm has already been suffered by the victim.

65. Due to the highly sensitive nature of Social Security numbers, theft of Social Security numbers in combination with other Personal Information (*e.g.*, name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. TIME Magazine quotes data security researcher Tom Stickley, who is employed by companies to find flaws in their computer systems, as stating, "If I have your name and your Social Security number and you haven't gotten a credit freeze yet, you're easy pickings."[18]

66. Further, malicious actors often wait months or years to use the Personal Information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen Personal Information, meaning individuals can be the victim of several cybercrimes stemming from a single data breach. Moreover, although elements of some of Plaintiff's and Class Members' data may have been compromised in other data breaches, the fact that the Data Breach centralizes the Personal Information and identifies the victims as MCNA Dental's current, former, or prospective customers materially increases the risk to Plaintiff and the Classes.

---

[18] Patrick Lucas Austin, *'It Is Absurd.' Data Breaches Show it's Time to Rethink How We Use Social Security Numbers, Experts Say*, TIME (Aug. 5, 2019), https://time.com/5643643/capital-one-equifax-data-breach-social-security/.

67. Theft of Personal Information is even more serious when it includes theft of PHI. A report published by the World Privacy Forum and presented at the U.S. Federal Trade Commission ("FCT") Workshop on Informational Injury describes what medical identity theft victims may experience:

- Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can affect the healthcare a person receives if the errors are not caught and corrected;
- Significant bills for medical goods and services neither sought nor received;
- Issues with insurance, co-pays, and insurance caps;
- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft;
- Serious life consequents resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime;
- As a result of improper and/or fraudulent medical debt reporting, victims may not qualify for mortgage or other loans and may experience other financial impacts;
- Phantom medical debt collection based on medical billing or other identity information;
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.[19]

68. The U.S. Government Accountability Office determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years." Moreover, there is often a significant lag time between when a person suffers harm due to theft of their Personal Information and when they discover the harm. Plaintiff and Class Members will

[19] Pam Dixon and John Emerson, The Geography of Medical Identity Theft, FTC.GOV (Dec. 12, 2017), http://www.worldprivacyforum.org/wp-content/uploads/2017/12/WPF_Geography_of_Medical_Identity_Theft_fs.pdf.

therefore need to spend time and money to continuously monitor their accounts for years to ensure the Personal Information obtained in the Data Breach is not used to harm them. Plaintiff and Class Members thus have been harmed in the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach. In other words, Plaintiff and Class Members have been harmed by the value of identity protection services they must purchase in the future to ameliorate the risk of harm they now face due to the Data Breach.

69. Plaintiff and Class Members have also been harmed and damaged in the amount of the market value of the hacker's access to their Personal Information that was permitted without authorization by MCNA Dental. This market value for access to Personal Information can be determined by reference to both legitimate and illegitimate markets for such information.

70. In sum, Plaintiff and Class Members were injured as follows: (a) theft of their Personal Information and the resulting loss of privacy rights in that information; (b) improper disclosure of their Personal Information; (c) loss or diminished value of their Personal Information; (d) the lost value of access to Plaintiff's and Class Members' Personal Information permitted by MCNA Dental; (e) the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach; (f) MCNA Dental's retention of profits attributable to Plaintiff's and Class Members' Personal Information that MCNA Dental failed to adequately protect; (g) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (h) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (i) overpayments to MCNA Dental for goods and services purchased, as Plaintiff and Class Members reasonably believed a portion of

the price they paid for those goods and services would fund reasonable security measures that would protect their Personal Information, which was not the case; and (j) nominal damages.

VI. CLASS ACTION ALLEGATIONS

NATIONWIDE CLASS

71. In accordance with Federal Rules of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiff brings this case as a class action on behalf of the following nationwide class (the "Nationwide Class"):

> **All [natural] persons residing in the United States whose Personal Information was maintained on MCNA Dental's systems that were compromised as a result of the breach announced by MCNA Dental on May 26, 2023.**

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

STATEWIDE SUBCLASS

72. In accordance with Federal Rules of Civil Procedure 23(b)(2), (b)(3), and (c)(4), Plaintiff brings this case as a class action and brings pertinent statutory or common law claims on behalf of the following Arkansas Subclass (the "Arkansas Subclass") defined as follows:

> **All natural persons residing in Arkansas whose Personal Information was maintained on MCNA Dental's systems that were compromised as a result of the breach announced by MCNA Dental on May 26, 2023.**

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

73. Excluded from the Nationwide Class and the Arkansas Subclass are MCNA Dental and MCNA Dental's parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which MCNA Dental has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting

out; all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

74. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

75. **Numerosity, Fed R. Civ. P. 23(a)(1):** The Nationwide Class and the Arkansas Subclass (the "Classes") are so numerous that joinder of all members is impracticable. MCNA Dental has identified millions of customers whose Personal Information may have been improperly accessed in the Data Breach. Those individuals' names and addresses are available from MCNA Dental's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods. On information and belief, there are at least a hundred Class Members in each Subclass, making joinder of all Subclass Members impracticable.

76. **Commonality and Predominance, Fed. R. Civ. P. 23(a)(2) and (b)(3):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include, but are not limited to, the following:

a) Whether MCNA Dental represented to Plaintiff and Class Members that MCNA Dental would protect Plaintiff's and the Class Members' Personal Information;

b) Whether MCNA Dental owed a duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Personal Information;

c) Whether MCNA Dental breached a duty to Plaintiff and Class Members to exercise due care in collecting, storing, and safeguarding their Personal Information;

d) Whether MCNA Dental has a contractual obligation to safeguard Plaintiff's and Class Members' Personal Information;

e) Whether MCNA Dental's conduct breached any contractual obligation to protect Plaintiff's and Class Members' Personal Information;

f) Whether MCNA Dental knew or should have known that its systems were vulnerable to a data breach;

g) Whether MCNA Dental was negligent in failing to implement reasonable and adequate security procedures and practices;

h) Whether MCNA Dental's security measures to protect its systems were reasonable in light of known legal requirements;

i) Whether MCNA Dental notified Plaintiff and Class Members that their Personal Information had been compromised as soon as practicable and without unreasonable delay after the Data Breach was discovered;

j) Whether the content of MCNA Dental's notice to Plaintiff and Class Members that their Personal Information had been compromised was adequate in light of known legal requirements;

k) Whether MCNA Dental violated its common law duties to Plaintiff and Class Members by failing to promptly notify Plaintiff and Class Members that their Personal Information had been compromised;

l) Whether MCNA Dental adequately addressed the vulnerabilities that permitted the Data Breach to occur;

m) Whether MCNA Dental's conduct injured Plaintiff and the Class Members;

n) Whether MCNA Dental's conduct violated HIPAA laws;

o) Whether MCNA Dental's conduct violated state consumer protection laws;

p) Whether MCNA Dental's conduct violated the laws of Florida and Arkansas;

q) Whether MCNA Dental's conduct violated state data privacy laws;

r) Whether MCNA Dental's conduct violated state data breach laws;

s) Whether Plaintiff and Class Members are entitled to actual damages and/or punitive damages as a result of MCNA Dental's wrongful conduct;

t) Whether Plaintiff and Class Members are entitled to restitution as a result of MCNA Dental's wrongful conduct; and

u) Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

77. Such issues are also appropriate for certification under Fed. R. Civ. P. 23(c)(4) because the claims present particular, common issues, the resolution of which would materially advance the resolution of this matter and the parties' interests therein.

78. **Typicality, Fed. R. Civ. P. 23(a)(3):** As to each Class and Subclass, Plaintiff's claims are typical of other Class Members' claims because Plaintiff and Class Members were subjected to the same allegedly unlawful conduct and damaged in the same way. Plaintiff's Personal Information was in MCNA Dental's possession at the time of the Data Breach and was

compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to those of other Class Members and Plaintiff seeks relief consistent with the relief of the Classes.

79. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Classes because Plaintiff is a member of the Classes and is committed to pursuing this matter against Defendant to obtain relief for the Classes. Plaintiff has no conflicts of interest with the Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class Members' interests.

80. **Superiority and Predominance, Fed. R. Civ. P. 23(b)(3):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class Members are relatively small compared to the burden and expense required to individually litigate their claims against MCNA Dental, and thus, individual litigation to redress MCNA Dental's wrongful conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action

device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

81. **Risk of Prosecuting Separate Actions:** This case is appropriate for certification because prosecuting separate actions by individual proposed Class Members would create the risk of inconsistent adjudications and incompatible standards of conduct for MCNA Dental or would be dispositive of the interests of members of the proposed Class.

82. **Ascertainability:** The Nationwide Class and Subclasses are defined by reference to objective criteria, and there is an administratively feasible mechanism to determine who fits within the Classes. The Nationwide Class and Subclasses consist of individuals who provided their Personal Information to MCNA Dental. Class membership can be determined using MCNA Dental's records.

83. **Injunctive and Declaratory Relief:** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Classes as a whole, making injunctive relief appropriate to the Classes as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

VII. CAUSES OF ACTION

COUNT I

Negligence
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

84. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 of above, as if fully set forth herein.

85. MCNA Dental collected sensitive Personal Information from Plaintiff and Class Members in connection with providing Dental Services.

86. MCNA Dental owed a duty to Plaintiff and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting their Personal Information in its possession from being compromised, lost, stolen, accessed, or misused by unauthorized persons. More specifically, this duty included, among other things: (a) designing, maintaining, and testing MCNA Dental's security systems to ensure that Plaintiff's and Class Members' Personal Information in MCNA Dental's possession was adequately secured and protected; (b) implementing processes that would detect a breach of its security system in a timely manner; (c) timely acting upon warnings and alerts, including those generated by its own security systems, regarding intrusions to its networks; and (d) maintaining data security measures consistent with industry standards.

87. MCNA Dental's duty to use reasonable care arose from several sources, including but not limited to those described herein.

88. MCNA Dental had common law duties to prevent foreseeable harm to Plaintiff and the Class Members. These duties existed because Plaintiff and Class Members were the foreseeable and probable victims of any inadequate security practices. Not only was it foreseeable that Plaintiff and Class Members would be harmed by MCNA Dental's failure to protect their Personal Information because hackers routinely attempt to steal such information and use it for nefarious purposes, MCNA Dental knew that it was more likely than not Plaintiff and other Class Members would be harmed if it allowed such a breach.

89. MCNA Dental's duty to use reasonable security measures also arose as a result of the special relationship that existed between MCNA Dental, on the one hand, and Plaintiff and Class Members, on the other hand. The special relationship arose because Plaintiff and Class Members entrusted MCNA Dental with their Personal Information and sensitive healthcare information.

MCNA Dental alone could have ensured that its security systems and data storage architecture were sufficient to prevent or minimize the Data Breach.

90. Defendant is covered by HIPAA (*see* 45 C.F.R. §160.102) and, as such is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

91. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. §160.103.

92. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

93. HIPAA requires that Defendant implements appropriate safeguards for this information.

94. MCNA Dental's duty also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. §45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Personal Information by companies such as MCNA Dental. Various FTC publications and data security breach orders further form the basis of MCNA Dental's duty. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

95. MCNA Dental admits that it has a responsibility to protect consumer data, that it is entrusted with this data, and that it did not live up to its responsibility to protect the Personal Information at issue here.

96. MCNA Dental knew or should have known that its computing systems and data storage architecture were vulnerable to unauthorized access and targeting by hackers for the purpose of stealing and misusing confidential Personal Information.

97. MCNA Dental also had a duty to safeguard the Personal Information of Plaintiff and Class Members and to promptly notify them of a breach because of state laws and statutes that require MCNA Dental to reasonably safeguard sensitive Personal Information, as detailed herein.

98. Timely, adequate notification was required, appropriate and necessary so that, among other things, Plaintiff and Class Members could take appropriate measures to freeze or lock their credit profiles, avoid unauthorized charges to their credit or debit card accounts, cancel or change usernames and passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, and take other steps to mitigate or ameliorate the damages caused by MCNA Dental's misconduct.

99. MCNA Dental breached the duties they owed to Plaintiff and Class Members described above and thus was negligent. MCNA Dental breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the Personal Information of Plaintiff and Class Members; (b) detect the Data Breach while it was ongoing; (c) maintain security systems consistent with industry standards during the period of the Data Breach; (d) comply with regulations protecting the Personal Information at issue during the period of the Data Breach; and (e) disclose in a timely and adequate

manner that Plaintiff and the Class Members' Personal Information in MCNA Dental's possession had been or was reasonably believed to have been, stolen or compromised.

100. But for MCNA Dental's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, their Personal Information would not have been compromised.

101. MCNA Dental's failure to take proper security measures to protect the sensitive Personal Information of Plaintiff and Class Members created conditions conducive to a foreseeable, intentional act, namely the unauthorized access of Plaintiff's and Class Members' Personal Information.

102. Plaintiff and Class Members were foreseeable victims of MCNA Dental's inadequate data security practices, and it was also foreseeable that MCNA Dental's failure to provide timely and adequate notice of the Data Breach would result in injury to Plaintiff and Class Members as described in this Complaint.

103. As a direct and proximate result of MCNA Dental's negligence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to

their Personal Information permitted by MCNA Dental; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages and other economic and non-economic harm.

COUNT II

Negligence *Per Se*
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

104. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 of above, as if fully set forth herein.

105. Defendant is covered by HIPAA (*see* 45 C.F.R. §160.102) and, as such, is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

106. These rules establish national standards for the protection of patient information, including protected health information, defined as "individually identifiable health information" which either "identifies the individual" or where there is a "reasonable basis to believe the information can be used to identify the individual," that is held or transmitted by a healthcare provider. *See* 45 C.F.R. §160.103.

107. HIPAA limits the permissible uses of "protected health information" and prohibits unauthorized disclosures of "protected health information."

108. HIPAA requires that Defendant implements appropriate safeguards for this information.

109. Section 5 of the Federal Trade Commission Act, 15 U.S.C. §45, also prohibits "unfair. . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by companies such as MCNA Dental of failing to use reasonable measures to protect Personal Information.

110. The FTC publications and orders also form the basis of MCNA Dental's duty.

111. MCNA Dental violated Section 5 of the FTC Act by failing to use reasonable measures to protect Personal Information and not complying with applicable industry standards. MCNA Dental's conduct was particularly unreasonable given the nature and amount of Personal Information it obtained, stored, and disseminated, and the foreseeable consequences of a data breach involving a company as large as MCNA Dental, including, specifically the damages that would result to Plaintiff and Class Members.

112. In addition, under state data security statutes, MCNA Dental had a duty to implement and maintain reasonable security procedures and practices to safeguard Plaintiff's and Class Members' Personal Information.

113. MCNA Dental's violation of HIPAA and Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

114. Plaintiff and Class Members are consumers within the class of persons Section 5 of the FTC Act was intended to protect.

115. The harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Classes.

116. MCNA Dental breached its duties to Plaintiff and Class Members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Personal Information.

117. Plaintiff and Class Members were foreseeable victims of MCNA Dental's violations of the HIPAA, the FTC Act, and state data security statutes. MCNA Dental knew or should have known that its failure to implement reasonable measures to protect and secure Plaintiff's and Class Members' Personal Information would cause damage to Plaintiff and Class Members.

118. But for MCNA Dental's violation of the applicable laws and regulations, Plaintiff's and Class Members' Personal Information would not have been accessed by unauthorized parties.

119. As a direct and proximate result of MCNA Dental's negligence *per se*, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by MCNA Dental; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach; lost benefit of their bargains and

overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT III

Breach of Confidence
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

120. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

121. Plaintiff and Class Members maintained a confidential relationship with MCNA Dental whereby MCNA Dental undertook a duty not to disclose to unauthorized parties the Personal Information that Plaintiff and Class Members provided to MCNA Dental. Such Personal Information was confidential and novel, highly personal and sensitive, and not generally known.

122. MCNA Dental knew Plaintiff's and Class Members' Personal Information was being disclosed in confidence and understood the confidence was to be maintained, including by expressly and implicitly agreeing to protect the confidentiality and security of the Personal Information it collected, stored, and maintained.

123. As a result of the Data Breach, there was an unauthorized disclosure of Plaintiff's and Class Members' Personal Information in violation of this understanding. The unauthorized disclosure occurred because MCNA Dental failed to implement and maintain reasonable safeguards to protect the Personal Information in its possession and failed to comply with industry-standard data security practices.

124. Plaintiff and Class Members were harmed by way of an unconsented disclosure of their confidential information to an unauthorized third party.

125. But for MCNA Dental's actions and inactions in violation of the parties' understanding of confidence, the Personal Information of Plaintiff and Class Members would not

have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. MCNA Dental's actions and inaction were the direct and legal cause of the theft of Plaintiff's and Class Members' Personal Information, as well as the resulting damages.

126. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of MCNA Dental's unauthorized disclosure of Plaintiff's and Class Members' Personal Information. MCNA Dental knew its computer systems and technologies for accepting, securing, and storing Plaintiff's and Class Members' Personal Information had serious security vulnerabilities because MCNA Dental failed to observe even basic information security practices or correct known security vulnerabilities.

127. As a direct and proximate result of MCNA Dental's breach of confidence, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach; lost benefit of their

bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

128. By collecting and storing this Personal Information and using it for commercial gain, MCNA Dental has a duty of care to use reasonable means to secure and safeguard this Personal Information to prevent disclosure and guard against theft of the Personal Information.

COUNT IV

Invasion of Privacy – Intrusion Upon Seclusion On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

129. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

130. Plaintiff reasonably expected that the Personal Information they shared with MCNA Dental would be protected and secured against access by unauthorized parties and would not be disclosed to or obtained by unauthorized parties or disclosed or obtained for any improper purpose.

131. MCNA Dental intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing their Personal Information without permission to a third party who then sold the Personal Information to other third-parties on the dark web.

132. By failing to keep Plaintiff's and Class Members' Personal Information secure, and disclosing Personal Information to unauthorized parties for unauthorized use, MCNA Dental unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, *inter alia*:

a) intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b) invading their privacy by improperly using Personal Information they provided to MCNA Dental for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c) failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

d) enabling the disclosure of their Personal Information without consent.

133. The Personal Information that was publicized during the Data Breach was highly sensitive, private, and confidential, as it included private financial and other Personal Information.

134. MCNA Dental's intrusions into Plaintiff's and Class Members' seclusion were substantial and would be highly offensive to a reasonable person, constituting an egregious breach of social norms.

135. As a direct and proximate result of MCNA Dental's invasions of privacy, Plaintiff and Class Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as mitigation measures because of MCNA Dental's Data Breach; lost benefit of their bargains and overcharges for services or products; nominal and general damages; and other economic and non-economic harm.

COUNT V

Breach of Contract
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

136. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

137. Plaintiff and Class Members entered into a valid and enforceable contract through which Defendant provided Dental Services to Plaintiff and Class Members. That contract included promises by Defendant to secure, safeguard, and not disclose Plaintiff's and Class Members' Personal Information.

138. Defendant's Privacy Policy memorialized the rights and obligations of Defendant and its patients and is an agreement between MCNA Dental and individuals who provided their Personal Information to MCNA Dental, including Plaintiff and Class Members.

139. Specifically, in its relevant Notice of Privacy Practices, MCNA Dental promises its patients that it is "committed to complying with the requirements and standards of the Health Insurance Portability and Accountability Act of 1996 (HIPAA)" and says that it is required by law to "maintain the privacy and security of your protected health information."[20] MCNA Dental also describes in its Privacy Policy the limited specific instances when it shares Personal Information and says that it will not otherwise share patients' information "unless you tell us we can in writing."[21]

[20] *See Our Privacy Practices*, MCNA Dental, https://www.mcna.net/en/privacy (updated June 2018)

[21] *Id.*

140. As part of its Privacy Policy, Defendant explicitly committed to protecting the privacy and security of Personal Information and promised to never share such information except under specified circumstances.

141. As described herein, MCNA Dental has repeatedly made other statements to Plaintiff and Class Members promising to ensure the security of their Personal Information.

142. Defendant promised to comply with all HIPAA standards, state and federal law, to ensure that Plaintiff's and Class Members' PII/PHI was protected, secured, kept private, and not disclosed.

143. Plaintiff and Class Members fully performed their obligations under their contracts with Defendant.

144. However, Defendant did not secure, safeguard, and/or keep private Plaintiff's and Class Members' Personal Information, and therefore Defendant breached its contract with Plaintiff and Class Members.

145. Defendant allowed third parties to access, copy, and/or transfer Plaintiff's and Class Members' Personal Information without permission. Therefore, Defendant breached the Privacy Policy with Plaintiff and Class Members.

146. Defendant's failure to satisfy its confidentiality and privacy obligations resulted in Defendant providing services to Plaintiff and Class Members that were of a diminished value.

147. As a result, Plaintiff and Class Members have been harmed, damaged, and/or injured as described herein.

148. In addition to monetary relief, Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, *inter alia*, strengthen its data security systems and

monitoring procedures, conduct periodic audits of those systems, and provide lifetime credit monitoring and identity theft insurance to Plaintiff and Class Members.

COUNT VI

Breach of Implied Contract
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

149. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

150. This Count is pleaded in the alternative to Count V above.

151. MCNA Dental provides medical services to Plaintiff and Class Members. Plaintiff and Class Members formed an implied contract with MCNA Dental regarding the provision of those services through their collective conduct.

152. Through MCNA Dental's provision of services, it knew or should have known that it must protect Plaintiff's and Class Members' confidential Personal Information in accordance with MCNA Dental's policies, practices, and applicable law, including the FTC Act and HIPAA.

153. As part of receiving services, Plaintiff and Class Members turned over valuable Personal Information to MCNA Dental. Accordingly, Plaintiff and Class Members bargained with Defendant to securely maintain and store their Personal Information.

154. Defendant violated these implied contracts by failing to employ reasonable and adequate security measures to secure Plaintiff's and Class Members' Personal Information.

155. Plaintiff and Class Members have been damaged by Defendant's conduct, including by incurring the harms and injuries arising from the Data Breach now and in the future.

COUNT VII

Unjust Enrichment
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

156. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

157. Plaintiff and Class Members have an interest, both equitable and legal, in the Personal Information about them that was conferred upon, collected by, and maintained by MCNA Dental and that was ultimately stolen in the MCNA Dental Data Breach.

158. MCNA Dental was benefited by the conferral upon it of the Personal Information pertaining to Plaintiff and Class Members and by its ability to retain, use, sell, and profit from that information. MCNA Dental understood that it was in fact so benefited.

159. MCNA Dental also understood and appreciated that the Personal Information pertaining to Plaintiff and Class Members was private and confidential and its value depended upon MCNA Dental maintaining the privacy and confidentiality of that Personal Information.

160. But for MCNA Dental's willingness and commitment to maintain its privacy and confidentiality, that Personal Information would not have been transferred to and entrusted with MCNA Dental.

161. Because of its use of Plaintiff's and Class Members' Personal Information, MCNA Dental sold more services and products than it otherwise would have sold. MCNA Dental was unjustly enriched by profiting from the additional services and products it was able to market, sell, and create to the detriment of Plaintiff and Class Members.

162. MCNA Dental also benefited through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Personal Information.

163. MCNA Dental also benefited through its unjust conduct in the form of the profits it gained through the use of Plaintiff's and Class Members' Personal Information.

164. It is inequitable for MCNA Dental to retain these benefits.

165. As a result of MCNA Dental's wrongful conduct as alleged in this Complaint (including, among things, its failure to employ adequate data security measures, its continued maintenance and use of the Personal Information belonging to Plaintiff and Class Members without having adequate data security measures, and its other conduct facilitating the theft of that Personal Information), MCNA Dental has been unjustly enriched at the expense of, and to the detriment of, Plaintiff and Class Members.

166. MCNA Dental's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiff's and Class Members' sensitive Personal Information, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

167. It is inequitable, unfair, and unjust for MCNA Dental to retain these wrongfully obtained benefits. MCNA Dental's retention of wrongfully obtained monies would violate fundamental principles of justice, equity, and good conscience.

168. The benefit conferred upon, received, and enjoyed by MCNA Dental was not conferred officiously or gratuitously, and it would be inequitable, unfair, and unjust for MCNA Dental to retain the benefit.

169. MCNA Dental's defective security and its unfair and deceptive conduct have, among other things, caused Plaintiff and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Personal Information and have caused Plaintiff and Class Members other damages as described herein.

170. Plaintiff and Class Members have no adequate remedy at law.

171. MCNA Dental is therefore liable to Plaintiff and Class Members for restitution or disgorgement in the amount of the benefit conferred on MCNA Dental as a result of its wrongful conduct, including specifically: the value to MCNA Dental of the Personal Information that was stolen in the Data Breach; the profits MCNA Dental received and is receiving from the use of that information; the amounts that MCNA Dental overcharged Plaintiff and Class Members for the use of MCNA Dental's products and services; and the amounts that MCNA Dental should have spent to provide reasonable and adequate data security to protect Plaintiff's and Class Members' Personal Information.

COUNT VIII

Violations of Arkansas' Deceptive Trade Practice Act
(Ark. Code Ann. §4-88-101, *et seq*.)
On Behalf of Plaintiff and Arkansas Subclass

172. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

173. MCNA Dental, Plaintiff, and the Arkansas Subclass Members are "persons" within the meaning of the Ark. Code Ann. §4-88-102(5).

174. The Dental Services Plaintiff and Arkansas Subclass Members received from MCNA Dental are "services" within the meaning of Ark. Code Ann. §4-88-102(7)

175. The Arkansas Deceptive Trade Practices Act ("Arkansas DTPA") makes unlawful "[d]eceptive and unconscionable trade practices," which include, but are not limited to, a list of enumerated items, including "[e]ngaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade[.]" Ark. Code Ann. §4-88-107(a)(10). The Arkansas DTPA also prohibits the following when utilized in connection with the sale or advertisement of any service: "(1) The act, use, or employment by any person of any deception, fraud, or false

pretense; or (2) The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission." Ark. Code Ann. §4-88-108.

176. MCNA Dental engaged in unfair and deceptive acts and practices that violated Ark. Code Ann. §4-88-107(a)(1), including:

a) Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and Subclass Members' PII, which was a direct and proximate cause of the Data Breach;

b) Failing to identify and remediate foreseeable security and privacy risks and sufficiently improve security and privacy measures despite knowing the risk of cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c) Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45, which was a direct and proximate cause of the Data Breach;

d) Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and Subclass Members' PII, including by implementing and maintaining reasonable security measures;

e) Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45;

f) Omitting, suppressing, and concealing the material fact that it did not properly secure Plaintiff's and Subclass Members' PII;

g) Failing to provide timely and accurate notice of the Data Breach as required by the Personal Information Protection Act, Ark. Code Ann. §4-110-101, *et seq.*; and

h) Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and Subclass Members' PII, including duties imposed by the FTC Act, 15 U.S.C. §45.

177. MCNA Dental's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of MCNA Dental's data security and ability to protect the confidentiality of consumers' PII.

178. MCNA Dental intended to mislead Plaintiff and Arkansas Subclass Members and induce them to rely on its misrepresentations and omissions.

179. MCNA Dental's unfair and deceptive acts and practices were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Arkansas Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

180. MCNA Dental acted intentionally, knowingly, and maliciously to violate Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Arkansas Subclass Members' rights. MCNA Dental's numerous past data breaches put it on notice that its security and privacy protections were inadequate.

181. Had MCNA Dental disclosed to Plaintiff and Subclass Members that its data systems were not secure and, thus, vulnerable to attack, MCNA Dental would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and

comply with the law. MCNA Dental was trusted with sensitive and valuable PII regarding millions of consumers, including Plaintiff and Subclass Members. MCNA Dental accepted the responsibility of protecting the data while keeping the inadequate state of its security controls secret from the public. Accordingly, Plaintiff and Subclass Members acted reasonably in relying on MCNA Dental's misrepresentations and omissions, the truth of which they could not have discovered.

182. As a direct and proximate result of MCNA Dental's unfair and deceptive acts and practices, Plaintiff and Arkansas Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for MCNA Dental's services; loss of the value of access to their PII; and the value of identity protection services made necessary by the Data Breach.

183. Plaintiff and Arkansas Subclass Members seek all monetary and non-monetary relief allowed by law, including actual damages; treble damages for MCNA Dental's knowing violations of the Arkansas DTPA; declaratory relief; attorneys' fees; and any other relief that is just and proper.

COUNT IV

Breach of Fiduciary Duty
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

184. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

185. As a condition of obtaining Dental Services from MCNA Dental, Plaintiff and Class Members gave MCNA Dental their Personal Information in confidence, believing that MCNA Dental would protect that information. Plaintiff and Class Members would not have provided MCNA Dental with this information had they known their information would not be adequately

protected. MCNA Dental's acceptance and storage of Plaintiff's and Class Members' Personal Information created a fiduciary relationship between MCNA Dental and Plaintiff and Class Members. In light of this relationship, MCNA Dental must act primarily for the benefit of its customers, which includes safeguarding and protecting Plaintiff's and Class Members' Personal Information. MCNA Dental has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship.

186. MCNA Dental breached that duty by failing to properly protect the integrity of the systems containing Plaintiff's and Class Members' Personal Information, failing to comply with the data security guidelines set forth by HIPAA, and otherwise failing to safeguard Plaintiff's and Class Members' Personal Information that it collected, retained, and stored.

187. As a direct and proximate result of MCNA Dental's negligence *per se*, Plaintiff and Members have been injured and are entitled to damages in an amount to be proven at trial. Such injuries include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Personal Information; illegal sale of the compromised Personal Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports, among other related activities; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Personal Information; lost value of access to their Personal Information permitted by MCNA Dental; the amount of the actuarial present value of ongoing high-quality identity defense and credit monitoring services made necessary as

mitigation measures because of MCNA Dental's Data Breach; and lost benefit of their bargains and overcharges for services or products.

COUNT V

Declaratory Judgment
On Behalf of Plaintiff and the Nationwide Class, or Alternatively, on Behalf of Plaintiff and the Arkansas Subclass

188. Plaintiff realleges and incorporates by reference the allegations contained in paragraphs 1-83 above, as if fully set forth herein.

189. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. The Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

190. An actual controversy has arisen in the wake of the MCNA Dental Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether MCNA Dental is currently maintaining data security measures adequate to protect Plaintiff and Class Members from further data breaches that compromise their Personal Information. Plaintiff and Class Members continue to suffer injury as a result of the compromise of their Personal Information and remain at imminent risk that further compromises of their Personal Information will occur in the future given the publicity around the Data Breach and the nature and quantity of the Personal Information stored by MCNA Dental.

191. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a) MCNA Dental continues to owe a legal duty to secure consumers' Personal Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes; and

b) MCNA Dental continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Personal Information.

192. The Court also should issue corresponding prospective injunctive relief requiring MCNA Dental to employ adequate security protocols consistent with law and industry standards to protect consumers' Personal Information.

193. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at MCNA Dental. The risk of another such breach is real, immediate, and substantial. If another data breach at MCNA Dental occurs, Plaintiff and Class Members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

194. The hardship to Plaintiff and Class Members, if an injunction does not issue, exceeds the hardship to MCNA Dental if an injunction is issued. Among other things, if another massive data breach occurs at MCNA Dental, Plaintiff and Class Members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to MCNA Dental of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and MCNA Dental has a pre-existing legal obligation to employ such measures.

195. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at MCNA Dental, thus eliminating the additional injuries that would result to Plaintiff and Class Members and the millions of consumers whose confidential information would be further compromised.

VIII. REQUEST FOR RELIEF

WHEREFORE, Plaintiff and Class Members demand judgment as follows:

A. Certification of the action as a Class Action Pursuant to Federal Rule of Civil Procedure 23, and appointment of Plaintiff as Class Representative and his counsel of record as Class Counsel;

B. That acts alleged herein be adjudged and decreed to constitute negligence and violations of the consumer protection laws of Florida and Arkansas;

C. A judgment against Defendant for the damages sustained by Plaintiff and the Classes defined herein, and for any additional damages, penalties, and other monetary relief provided by applicable law;

D. An order providing injunctive and other equitable relief as necessary to protect the interests of the Classes, including, but not limited to:

1. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
2. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;
3. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;
4. Ordering that Defendant segment consumer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, unauthorized third parties cannot gain access to other portions of Defendant's systems;

5. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner consumer data not necessary for their provisions of services;

6. Ordering that Defendant conduct regular database scanning; and

7. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

E. By awarding Plaintiff and Class Members pre-judgment and post-judgment interest as provided by law, and that such interest be awarded at the highest legal rate from and after the date of service of the Complaint in this action;

F. The costs of this suit, including reasonable attorney fees; and

G. Such other and further relief as the Court deems just and proper.

IX. DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all those similarly situated, hereby requests a jury trial, pursuant to Federal Rule of Civil Procedure 38, on any and all claims so triable.

DATED: June 29, 2023

Respectfully submitted,

/s/ Jason H. Alperstein

Jason H. Alperstein (FBN 64205)
Zachary S. Bower (FBN 17506)
CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.
2222 Ponce de Leon
Miami, Florida 33134
Phone: (973) 994-1700
jalperstein@carellabyrne.com
zbower@carellabyrne.com

James E. Cecchi*
Kevin G. Cooper*
Jordan M. Steele*
CARELLA, BYRNE, CECCHI, OLSTEIN, BRODY & AGNELLO, P.C.

5 Becker Farm Road
Roseland, New Jersey 07068
Phone: (973) 994-1700
jcecchi@carellabyrne.com
kcooper@carellabyrne.com
jsteele@carellabyrne.com

Dorothy P. Antullis (FBN 890421)
Alexander C. Cohen (FBN 1002715)
ROBBINS GELLER RUDMAN & DOWD LLP
225 NE Mizner Boulevard, Suite 720
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
dantullis@rgrdlaw.com
acohen@rgrdlaw.com

Counsel for Plaintiff and the Proposed Class

**To be admitted pro hac vice*